ON MAXIMAL CURVES IN CHARACTERISTIC TWO

MIRIAM ABDÓN AND FERNANDO TORRES

ABSTRACT. The genus g of an $\mathbb{F}_{q^2}$-maximal curve satisfies $g = g_1 := q(q-1)/2$ or $g \leq g_2 := \lfloor (q-1)^2/4 \rfloor$. Previously, $\mathbb{F}_{q^2}$-maximal curves with $g = g_1$ or $g = g_2$, q odd, have been characterized up to $\mathbb{F}_{q^2}$-isomorphism. Here it is shown that an $\mathbb{F}_{q^2}$-maximal curve with genus g_2, q even, is $\mathbb{F}_{q^2}$-isomorphic to the nonsingular model of the plane curve $\sum_{i=1}^{t} y^{q/2^i} = x^{q+1}$, $q = 2^t$, provided that $q/2$ is a Weierstrass non-gap at some point of the curve.

1. A projective geometrically irreducible nonsingular algebraic curve defined over $\mathbb{F}_{q^2}$, the finite field with q^2 elements, is called $\mathbb{F}_{q^2}$-*maximal* if the number of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound

$$q^2 + 1 + 2qg \,,$$

where g is the genus of the curve. Maximal curves became useful in Coding Theory after Goppa's paper [Go], and have been intensively studied in [Sti-X], [Geer-Vl1] (see also the references therein), [Geer-Vl2], [FT1], [FGT], [FT2], [GT], [CHKT], [CKT1], [G-Sti-X] and [CKT2].

The key property of a $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ is the existence of a base-point-free linear system $\mathcal{D}_{\mathcal{X}} := |(q+1)P_0|$, $P_0 \in \mathcal{X}(\mathbb{F}_{q^2})$, defined on $\mathcal{X}$ such that [FGT, §1]

(1.1) $qP + \mathrm{Fr}_{\mathcal{X}}(P) \in \mathcal{D}_{\mathcal{X}}$,
(1.2) $\mathcal{D}_{\mathcal{X}}$ is simple,
(1.3) $\dim(\mathcal{D}_{\mathcal{X}}) \geq 2$,

where $\mathrm{Fr}_{\mathcal{X}}$ denotes de Frobenius morphism on $\mathcal{X}$ relative to $\mathbb{F}_{q^2}$. Then via Stöhr-Voloch's approach to the Hasse-Weil bound [SV] one can establish arithmetical and geometrical properties of maximal curves. In addition, Property (1.2) allows the use of Castelnuovo's genus bound in projective spaces [Cas], [ACGH, p. 116], [Ra, Corollary 2.8]. In particular, the following relation involving the genus g of $\mathcal{X}$ and $n := \dim(\mathcal{D}_{\mathcal{X}}) - 1$ holds [FGT, p. 34]

(1)
$$2g \leq \begin{cases} (q - n/2)^2/n & \text{if } n \text{ is even}, \\ ((q - n/2)^2 - 1/4)/n & \text{otherwise}. \end{cases}$$

It follows that

$$g \leq g_1 := q(q-1)/2 \,,$$

1991 Math. Subj. Class.: Primary 11G, Secondary 14G.

which is a result pointed out by Ihara [Ih]. As a matter of fact, the so called *Hermitian curve*, i.e. the plane curve $\mathcal{H}$ defined by

$$Y^q Z + Y Z^q = X^{q+1} \, ,$$

is the unique $\mathbb{F}_{q^2}$-maximal curve whose genus is g_1 up to $\mathbb{F}_{q^2}$-isomorphism [R-Sti]. More-over, $\mathcal{H}$ is the unique $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ such that $\dim(\mathcal{D}_{\mathcal{X}}) = 2$ [FT2, Thm 2.4]. Therefore, if $g < g_1$, then $\dim(\mathcal{D}_{\mathcal{X}}) \geq 3$ and hence (1) implies [Sti-X], [FT1]

$$g \leq g_2 := \lfloor (q-1)^2/4 \rfloor \, .$$

If q is odd, there is a unique $\mathbb{F}_{q^2}$-maximal curve, up to $\mathbb{F}_{q^2}$-isomorphism, whose genus belongs to the interval $](q-1)(q-2)/4, (q-1)^2/4]$, namely the nonsingular model of the plane curve

$$y^q + y = x^{(q+1)/2} \, ,$$

whose genus is $g_2 = (q-1)^2/4$ [FGT, Thm. 3.1], [FT2, Prop. 2.5].

The purpose of this paper is to extend this result to even characteristic provided that a condition on Weierstrass non-gaps is satisfied. For q even, say $q = 2^t$, notice that $g_2 = q(q-2)/4$ and that the nonsingular model of the plane curve

(2)
$$\sum_{i=1}^{t} y^{q/2^i} = x^{q+1}$$

is an $\mathbb{F}_{q^2}$-maximal curve of genus g_2.

Theorem. *Let q be even, $\mathcal{X}$ a $\mathbb{F}_{q^2}$-maximal curve of genus g having both properties:*

1. *$(q-1)(q-2)/4 < g \leq g_2 = q(q-2)/4$, and*
2. *There exists $P \in \mathcal{X}$ such that $q/2$ is a Weierstrass non-gap at P.*

Then $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to the nonsingular model of the plane curve defined by Eq. (2). In particular, $g = g_2$.

Let $\mathcal{X}$ be a $\mathbb{F}_{q^2}$-maximal of genus $g \in](q-1)(q-2)/4, q(q-2)/4]$, q even, and $P \in \mathcal{X}$. We have that $P \in \mathcal{X}(\mathbb{F}_{q^2})$ if $q/2$ is a Weierstrass non-gap at P, see Corollary 2. Now, on the one hand, from Corollary 1, $\mathcal{X}$ only admits two types of Weierstrass semigroups at $\mathbb{F}_{q^2}$-rational points, namely either semigroups of type $\langle q/2, q+1 \rangle$ or semigroups of type $\langle q-1, q, q+1 \rangle$. On the other hand, from Proposition 3, $\mathcal{X}$ satisfies the second hypothesis of the theorem provided that $\mathcal{X}$ is $\mathbb{F}_{q^2}$-covered by $\mathcal{H}$. Therefore, if there existed a $\mathbb{F}_{q^2}$-maximal curve of genus $g \in](q-1)(q-2)/4, q(q-2)/4]$ for which the Weierstrass semigroup at any $\mathbb{F}_{q^2}$-rational point is $\langle q-1, q, q+1 \rangle$, then such a curve could not be $\mathbb{F}_{q^2}$-covered by the Hermitian curve. As far as we know, the existence of maximal curves not covered by the Hermitian is an open problem. We notice that the nonsingular model $\mathcal{X}$ of the plane curves $y^q + y = x^m$, m a divisor of $q+1$, have been characterized as those curves such that $m_1(P)n = q+1$ for some $P \in \mathcal{X}(\mathbb{F}_{q^2})$, where $m_1(P)$ stands for the first positive

Weierstrass non-gap at P and $n = \dim(\mathcal{X}) - 1$; see [FGT, §2]. Moreover, the hypothesis on Weierstrass non-gaps cannot be relaxed, cf. [FT2, p. 37], [CHKT, Remark 4.1(ii)].

We prove the theorem by using some properties of maximal curves stated in [FGT], [FT2] and [CKT1], Castelnuovo's genus bound in projective spaces, and Frobenius orders which were introduced by Stöhr and Voloch [SV]. For basic facts on Weierstrass point theory and Frobenius orders the reader is referred to [SV].

2. Proof of the Theorem. Let $\mathcal{X}$ be a $\mathbb{F}_{q^2}$-maximal curve of genus g large enough. The starting point of the proof is the computation of some invariants for the following linear systems:

$$\mathcal{D} := \mathcal{D}_{\mathcal{X}} = |(q+1)P_0| \quad \text{and} \quad 2\mathcal{D} := 2\mathcal{D}_{\mathcal{X}} = |2(q+1)P_0|\,,$$

where $P_0 \in \mathcal{X}(\mathbb{F}_{q^2})$. For $P \in \mathcal{X}$, let $(m_i(P) : i \in \mathbb{N}_0)$ be the strictly increasing sequence that enumerates the Weierstrass semigroup $H(P)$ at P.

Lemma 1. *Let $\mathcal{X}$ be a $\mathbb{F}_{q^2}$-maximal curve of genus g such that*

$$(q-1)(q-2)/4 < g \le (q-1)^2/4\,.$$

Then the following properties hold:

1. *We have $\dim(\mathcal{D}) = 3$.*
2. *If $P \in \mathcal{X}(\mathbb{F}_{q^2})$, then the $(\mathcal{D}, P)$-orders are $0, 1, q+1-m_1(P)$ and $q+1$. If $P \notin \mathcal{X}(\mathbb{F}_{q^2})$, then the set of $(\mathcal{D}, P)$-orders contains the elements $q - m_i(P)$, $i = 0, 1, 2$.*
3. *We have $\dim(2\mathcal{D}) = 8$.*

Proof. (1) From Iq. (1) and the lower bound on g it follows that $\dim(\mathcal{D}) \le 3$ (indeed, we obtain this result for $(q-1)(q-2)/6 < g$. If we had $\dim(\mathcal{D}) = 2$, then from [FT2, Thm. 2.4] it would follow $g = q(q-1)/2$, contradiction. Thus $\dim(\mathcal{D}) = 3$.

(2) See [FGT, Prop. 1.5(ii)(iii)].

(3) An easy computation shows that $2m_3(P_0) \ge 8$, since $m_2(P_0) = q$ and $m_3(P_0) = q + 1$ [FGT, Prop. 1.5(iv)]. Hence $\dim(2\mathcal{D}) \ge 8$; the equality follows from Castelnuovo's genus bound and the lower bound on g. □

Corollary 1. *Let $\mathcal{X}$ be as in the previous lemma and suppose that q is even, $q > 4$.*

1. *For $P \in \mathcal{X}(\mathbb{F}_{q^2})$,*
   (i) the $(\mathcal{D}, P)$ orders are either $0, 1, 2, q+1$ or $0, 1, q/2+1, q+1$;
   (ii) either $m_1(P) = q - 1$ or $m_1(P) = q/2$. Equivalently, the first three positive Weierstrass non-gaps at P are either $q-1, q, q+1$ or $q/2, q, q+1$.
2. *For $P \notin \mathcal{X}(\mathbb{F}_{q^2})$, the $(\mathcal{D}, P)$-orders are either $0, 1, 2, q$ or $0, 1, q/2, q$.*

Proof. (1) Let $P \in \mathcal{X}(\mathbb{F}_{q^2})$ and set $j := q + 1 - m_1(P)$. By Lemma 1(2), it is enough to prove (i). From that result and the definition of $2\mathcal{D}$, the following set

$$O := \{0, 1, 2, j, j+1, 2j, q+1, q+2, q+1+j, 2q+2\}$$

is contained in the set of $(2\mathcal{D}, P)$-orders. Since $\dim(2\mathcal{D}) = 8$ (see Lemma 1(3)), $\#O \leq 9$. We observe that $j < q$: otherwise $g = 0$. So if $j > 2$, then $2j = q + 2$, as q is even, and the result follows.

(2) From Lemma 1(1) and [FGT, Thm. 1.4(ii)(iii)], the $(\mathcal{D}, P)$-orders are $0, 1, j = j(P)$ and q with $2 \leq j \leq q-1$. We claim that $j < q-1$. Otherwise $(q-1)P + D_P \sim qP + \mathrm{Fr}_{\mathcal{X}}(P)$, with $P \notin \mathrm{Supp}(D_P)$ and so $\mathcal{X}$ would be hyperelliptic; then $1 + q^2 + 2qg \leq 2(1 + q^2)$ and hence $(q-1)(q-2)/4 < g \leq q/2$, a contradiction since we have assumed $q > 4$. Now, the following set

$$\{0, 1, 2, j, j+1, 2j, q, q+1, q+j, 2q\}$$

is contained in the set of $(2\mathcal{D}, P)$-orders and the result follows as in the proof of item (1). $\qquad\square$

Corollary 2. *Let $\mathcal{X}$ be as in Lemma 1 and suppose that q is even, $q > 4$. Suppose also that $q/2$ is a Weierstrass non-gap at $P \in \mathcal{X}$. Then $P \in \mathcal{X}(\mathbb{F}_{q^2})$.*

Proof. Suppose that $P \notin \mathcal{X}(\mathbb{F}_{q^2})$. Let $x \in \bar{\mathbb{F}}_{q^2}(\mathcal{X})$ such that $\mathrm{div}_\infty(x) = q/2P$. Let $e := v_{\mathrm{Fr}_{\mathcal{X}}(P)}(x - x(\mathrm{Fr}_{\mathcal{X}}(P)))$. Then $\mathrm{div}(x - x(\mathrm{Fr}_{\mathcal{X}}(P)) = e\mathrm{Fr}_{\mathcal{X}}(P) + D - q/2P$ with $P, \mathrm{Fr}_{\mathcal{X}}(P) \notin \mathrm{Supp}(D)$. ¿From Property (1.1), both $e + 1$ and $2e + 1$ are $(\mathcal{D}, \mathrm{Fr}_{\mathcal{X}}(P))$-orders. Since $\mathrm{Fr}_{\mathcal{X}}(P) \notin \mathcal{X}(\mathbb{F}_{q^2})$ and $e \geq 1$, from Corollary 1(2) follows that $q = 3$, a contradiction. $\qquad\square$

Now, for $q > 4$ the theorem follows from the proposition below. The case $q = 4$ is considered in §4.

Proposition 1. *Let $\mathcal{X}$ be a projective geometrically irreducible nonsingular algebraic curve over $\mathbb{F}_{q^2}$, q even. The following statements are equivalent:*

1. *The curve $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to the non-singular model of the plane curve given by Eq. (2).*
2. *The curve $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal of positive genus, $\dim(\mathcal{D}_{\mathcal{X}}) = 3$, and there exists $P_0 \in \mathcal{X}(\mathbb{F}_{q^2})$ such that $q/2$ is a Weierstrass non-gap at P_0.*
3. *The curve is $\mathbb{F}_{q^2}$-maximal and there exists $P_1 \in \mathcal{X}(\mathbb{F}_{q^2})$ such that for $\mathcal{D} := \mathcal{D}_{\mathcal{X}} = |(q+1)P_1|$, the following holds:*
    (i) the $(\mathcal{D}, P_1)$-orders are $0, 1, q/2+1, q+1$;
    (ii) the $(\mathcal{D}, P)$-orders are $0, 1, 2, q+1$ if $P \in \mathcal{X}(\mathbb{F}_{q^2}) \setminus \{P_1\}$;
    (iii) the $(\mathcal{D}, P)$-orders are $0, 1, 2, q$ if $P \in \mathcal{X} \setminus \mathcal{X}(\mathbb{F}_{q^2})$;
    (iv) the $\mathbb{F}_{q^2}$-Frobenius orders of $\mathcal{D}$ are $0, 1, q$.

3. Proof of Proposition 1. Throughout this section we assume $q \geq 4$ since the case $q = 2$ is trivial.

$(1) \Rightarrow (2)$: The non-singular model of (2) is $\mathbb{F}_{q^2}$-covered by the Hermitian curve, and so it is maximal by [La, Prop. 6]. The unique point P_0 over $x = \infty$ is $\mathbb{F}_{q^2}$-rational and $q/2$

and $q + 1$ are Weierstrass non-gaps at P_0. Since the genus of the curve is $q(q - 2)/2$, it follows that $\dim(|(q + 1)P_0|) = 3$.

$(2) \Rightarrow (3)$: This implication is a particular case of [FT2, p. 38]; for the sake of completeness we write the proof. Take $P_1 = P_0$. Then $m_1(P_0) = q/2$, $m_2(P_0) = q$ and $m_3(P_0) = q + 1$, cf. Corollary 1(1)(ii). The case $P = P_0$ follows from Lemma 1(2). Let $P \in \mathcal{X} \setminus \{P_0\}$. Let $x \in \mathbb{F}_{q^2}(\mathcal{X})$ such that $\mathrm{div}_\infty(x) = m_1(P_0)P_0$. Then $e_P := v_P(x - x(P))$ and $2e_P$ are $(\mathcal{D}, P)$-orders. We claim that $e_P = 1$; otherwise $0, 1, e_P$, and $2e_P$ would be $(\mathcal{D}, P)$-orders and hence, by [FGT, Thm. 1.4(ii)] and being q even, we would have $e_P = q/2$ and $P \notin \mathcal{X}(\mathbb{F}_{q^2})$. Therefore $q/2P \sim q/2P_0$ and from Property (1.1) (and since the genus of $\mathcal{X}$ is positive) we would have $\mathrm{Fr}_\mathcal{X}(P) = P_0$, a contradiction. Thus, by [FGT, Thm. 1.4(ii)(iii)], the $(\mathcal{D}, P)$-orders are $0, 1, 2$ and $q + 1$ (resp. $0, 1, 2$, and q) if $P \in \mathcal{X}(\mathbb{F}_{q^2})$ (resp. $P \notin \mathcal{X}(\mathbb{F}_{q^2})$). Finally, the assertion on $\mathbb{F}_{q^2}$-Frobenius orders follows from $\dim(\mathcal{D}) = 3$ and [FT2, §2.2].

$(3) \Rightarrow (1)$: By Lemma 1(2), $m_1(P_1) = q/2$, $m_2(P_1) = q$ and $m_3(P_1) = q + 1$. Let $x, y \in \mathbb{F}_{q^2}(\mathcal{X})$ such that

$$\mathrm{div}_\infty(x) = q/2P_1 , \qquad \text{and} \qquad \mathrm{div}_\infty(y) = (q + 1)P_1 .$$

Then $\mathcal{X}$ admits a $\mathbb{F}_{q^2}$-plane model of type

$$(3) \qquad\qquad x^{q+1} + ay^{q/2} + \sum_{i=0}^{q/2-1} A_i(x)y^i = 0 ,$$

where $a \in \mathbb{F}_{q^2}^*$ and $A_i(x) \in \mathbb{F}_{q^2}[x]$ with $\deg(A_i(x)) \leq q - 2i$, $i = 0, \ldots, q/2 - 1$. This equation is usually referred to as the *Weierstrass canonical form over $\mathbb{F}_{q^2}$* of $\mathcal{X}$, see e.g. [K, Lemma 3] and the references therein.

Next we use x as a separating variable of $\mathbb{F}_{q^2}(\mathcal{X}) \mid \mathbb{F}_{q^2}$, and denote by $D^i := D_x^i$ the ith Hasse derivative with respect to x. Properties of these operators can be found e.g. in [He, §3]. In particular, we recall the following facts: For $z, w \in \bar{\mathbb{F}}_{q^2}(\mathcal{X})$,

(H1) $\quad D^i(z + w) = D^i(z) + D^i(w)$,
(H2) $\quad D^i(zw) = \sum_{j=0}^i D^{i-j}(z)D^j(w)$,
(H3)

$$D^i z^{2j} = \begin{cases} (D^{i/2}z^j)^2 & \text{if } i \text{ is even}, \\ 0 & \text{otherwise} . \end{cases}$$

Then, for q' a power of two, (H3) implies:

(H3')

$$D^i z^{q'} = \begin{cases} (D^{i/q'}z)^{q'} & \text{if } i \equiv 0 \pmod{q'}, \\ 0 & \text{otherwise} . \end{cases}$$

Now, the morphism associated to $\mathcal{D}$ is given by $(1 : x : x^2 : y)$. Since the $\mathcal{D}$-orders are $0, 1, 2$ and q, for $i = 3, \ldots, q - 1$, we have (see [SV, p. 5])

$$
\det \begin{pmatrix} 1 & x & x^2 & y \\ 0 & 1 & 0 & Dy \\ 0 & 0 & 1 & D^2y \\ 0 & 0 & 0 & D^iy \end{pmatrix} = D^iy = 0 \,.
$$

We also have

$$
\det \begin{pmatrix} 1 & x^{q^2} & x^{2q^2} & y^{q^2} \\ 1 & x & x^2 & y \\ 0 & 1 & 0 & Dy \\ 0 & 0 & 1 & D^2y \end{pmatrix} = 0 \,,
$$

or equivalently,

$$
(4) \qquad y + y^{q^2} + (x + x^{q^2})Dy + (x^2 + x^{2q^2})D^2y = 0 \,,
$$

since the $\mathbb{F}_{q^2}$-Frobenius orders of $\mathcal{D}$ are $0, 1$ and q (see [SV, Prop. 2.1]).

Claim 1. Eq. (3) can be simplified to

$$
(5) \qquad \sum_{i=1}^{t} a_i y^{q/2^i} + b = x^{q+1} \,,
$$

where $a_1, \ldots, a_t, b \in \bar{\mathbb{F}}_{q^2}$ with $a_t \in \mathbb{F}_{q^2}$.

Let us first show how this claim implies Proposition 1(1). To do so, let $\alpha \in \bar{\mathbb{F}}_{q^2}$ such that

$$
\sum_{i=1}^{t} a_i \alpha^{q/2^i} = b \,.
$$

Then, with $z := y + \alpha$, the curve $\mathcal{X}$ is $\bar{\mathbb{F}}_{q^2}$-isomorphic to the non-singular model of the curve defined by

$$
\sum_{i=1}^{t} a_i z^{q/2^i} = x^{q+1} \,.
$$

Fact 1. The element a_t can be assumed to be equal to one. If so, then

1. $a_{t-1} = a_1^{-2}$.
2. $a_i = a_{t-1}^{2^{t-i}-1}$, $i = 1, \ldots, t - 1$. In particular, $a_i \in \mathbb{F}_{q^2}^*$ for each i.
3. $\alpha \in \mathbb{F}_{q^2}$.

Proof. (*Fact* 1) From Eq. (5), we have

$$
a_t Dy = x^q \qquad \text{and} \qquad a_t^3 D^2y = a_{t-1}x^{2q} \,,
$$

and so $a_t \neq 0$. Hence we can assume $a_t = 1$ via the automorphism $(x, y) \mapsto (x, a_t y)$. Now from Eq. (4) we obtain

$$y + y^{q^2} + x^{q+1} + (x^{q+1})^q + a_{t-1}((x^{q+1})^2 + (x^{q+1})^{2q}) = 0.$$

This relation together with Eq. (5) imply

$$(1 + a_{t-1}a_1^{2q})y^{q^2} + \sum_{i=1}^{t-1}(a_i^q + a_{t-1}a_{i+1}^{2q})y^{q^2/2^i} + (1 + a_{t-1}a_1^2)y^q +$$

$$\sum_{i=1}^{t-1} a_i + (a_{t-1}a_{i+1}^2)y^{q/2^i} + b + b^q + a_{t-1}(b^2 + b^{2q}) = 0.$$

Therefore, as $v_{P_1}(y) < 0$, the following identities hold

(i) $1 + a_{t-1}a_1^{2q} = 0$,
(ii) $1 + a_{t-1}a_1^2 = 0$,
(iii) $a_i + a_{t-1}a_{i+1}^2 = 0$, $i = 1, \ldots, t-1$,
(iv) $a_i^q + a_{t-1}a_{i+1}^{2q} = 0$, $i = 1, \ldots, t-1$,   and,
(v) $b + b^q + a_{t-1}(b^2 + b^{2q}) = 0$.

¿From (i) and (iii) follow Items 1 and 2. To see Item 3 we replace b by $\sum_{i=1}^{t} a_i \alpha^{q/2^i}$ in (v). After some computations and using (i)–(iv) we find that $\alpha + \alpha^{q^2} = 0$ and the proof of Fact 1 is complete.   □

Consequently, the automorphism $(x, y) \mapsto (x, y + \alpha)$ is indeed defined over $\mathbb{F}_{q^2}$. Finally let $x_1 := a_1^{-1}x$ and $y_1 := a_{t-1}z$. Then from Fact 1 we obtain

$$\sum_{i=1}^{t} y_1^{q/2^i} = x_1^{q+1},$$

which shows Proposition 1(1).

(*Proof of Claim 1.*) Suppose that x and y satisfy a relation of type

(6) $$x^{q+1} + ay^{q/2} + \sum_{i=0}^{2^{s-2}-1} A_{i2^{t+1-s}}(x)y^{i2^{t+1-s}} + \sum_{i=s}^{t} a_i y^{2^{t-i}} = 0,$$

where $a \in \mathbb{F}_{q^2}^*$, $2 \leq s \leq t+1$, and $a_i \in \mathbb{F}_{q^2}$ for each i. Recall that $q = 2^t$ and notice that Eq. (3) provides such a relation for $s = t+1$.

Fact 2. For $2 \leq s \leq t+1$, we have

1. $A_{(2i+1)2^{t+1-s}}(x) = 0$, $i \geq 1$.
2. $A_{2^{t+1-s}}(x) \in \mathbb{F}_{q^2}$.

Proof. (*Fact 2*) By applying $D^{2^{t+1-s}}$ to Eq (6) and using properties (H1)–(H3) and (H3') above we have that

$$(7) \qquad a'\Gamma + \sum_{i=0}^{2^{s-2}-1} \Delta_i + \sum_{i=0}^{2^{s-2}-1} A_{i2^{t+1-s}}(x)(Dy^i)^{2^{t+1-s}} + \Lambda + \Psi = 0,$$

where

$$\Gamma := \begin{cases} (Dy)^{2^{t-1}} & \text{if } s = 2, \\ 0 & \text{otherwise}; \end{cases}$$

$$\Delta_i := \begin{cases} D(A_i(x))y^i & \text{if } s = t+1, \\ \sum_{j=0}^{2^{t-s}-1} D^{2^{t+1-s}-2j}(A_{i2^{t+1-s}}(x))D^{2j}(y^{i2^{t+1-s}}) & \text{otherwise}; \end{cases}$$

$$\Lambda := \begin{cases} 0 & \text{if } s = t+1, \\ (D^2y)^{2^{t-s}} & \text{otherwise}; \end{cases}$$

and

$$\Psi := \begin{cases} x^q & \text{if } s = t+1, \\ 0 & \text{otherwise}. \end{cases}$$

Since $D^{2^{t+1-s}}(y^{i2^{t+1-s}}) = (Dy^i)^{2^{t+1-s}}$, Eq. (7) becomes

$$(8) \qquad a'\Gamma + \sum_{i=0}^{2^{s-2}-1} \Delta_i + F(Dy)^{2^{t+1-s}} + \Lambda + \Psi = 0,$$

where

$$F := \sum_{i=0}^{2^{s-2}-1} A_{(2i+1)2^{t+1-s}}(x)y^{i2^{t+2-s}}.$$

Next we show that $v_{P_1}(F) = 0$ (*). This will imply Fact 2 since

$$v_{P_1}(F) = \min\{v_{P_1}(A_{(2i+1)2^{t+1-s}}(x)y^{i2^{t+2-s}}) : i = 0, \dots, 2^{s-2} - 1\}.$$

To see (*), we first compute $v_{P_1}(Dy)$ and $v_{P_1}(D^2y)$. For a local parameter t at P_1, we have

$$v_{P_1}(Dy) = v_{P_1}(dy/dt) - v_{P_1}(dx/dt) = -q - 2 - v_{P_1}(dx/dt).$$

To calculate $v_{P_1}(dx/dt)$, we use the fact that $x : \mathcal{X} \to \mathbb{P}^1(\bar{\mathbb{F}}_{q^2})$ is totally ramified at P_1, and that $v_P(x - x(P)) = 1$ for each $P \in \mathcal{X} \setminus \{P_1\}$ (cf. proof of (2) $\Rightarrow$ (3)). We have then $v_{P_1}(dx/dt) = 2g - 2 = q^2/2 - q - 2$ and so

$$v_{P_1}(Dy) = -q^2/2.$$

Now we compute $v_{P_1}(D^2y)$ from Eq. (4). In fact, as

$$v_{P_1}(y + y^{q^2}) = -q^2(q+1) < v_{P_1}(Dy(x + x^{q^2})) = -q^2(q+1)/2,$$

then $v_{P_1}((x^2 + x^{2q^2})D^2y) = v_{P_1}(y + y^{q^2})$ and so

$$v_{P_1}(D^2y) = -q^2 \,.$$

If $s = t + 1$, then Eq. (8) reads

$$\sum_{i=0}^{q/2-1} D(A_i(x))y^i + FDy + x^q = 0 \,.$$

Thus we have

$$v_{P_1}(F) + v_{P_1}(Dy) = v_{P_1}(x^q) \,,$$

since $v_{P_1}(\sum_{i=0}^{q/2-1} D(A_i(x))y^i) > v_{P_1}(x^q)$ as $\deg(A_i(x)) \le q - 2i$ for each i. Then $(*)$ follows because $v_{P_1}(x^q) = -q^2/2$.

Let $3 \le s \le t$. Then Eq. (8) reads

$$\sum_{i=0}^{2^{s-2}-1} \Delta_i + F(Dy)^{2^{t+1-s}} + (D^2y)^{2^{t-s}} = 0 \,.$$

Consequently, as $v_{P_1}(\sum_{i=0}^{2^{s-2}-1} \Delta_i) > 2^{t-s}v_{P_1}(D^2y)$, we have that

$$v_{P_1}(F) + 2^{t+1-s}v_{P_1}(Dy) = 2^{t-s}v_{P_1}(D^2y) \,,$$

and the proof follows for $s \ge 3$.

Finally, let $s = 2$. Then Eq. (8) reads

$$a'(Dy)^{q/2} + \Delta_0 + F(Dy)^{q/2} + (D^2y)^{q/4} = 0 \,.$$

Then as above we have

$$v_{P_1}(F) + qv_{P_1}(Dy)/2 = qv_{P_1}(D^2y)/4 \,,$$

and the proof of Fact 2 is complete. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Applying Fact 2 for $s = t + 1, \dots, 2$, we reduce Eq. 3 to

$$(9) \qquad\qquad x^{q+1} + ay^{q/2} + A_0(x) + \sum_{i=2}^{t} a_i y^{q/2^i} = 0 \,,$$

where $A_0(x) = \sum_{i=0}^{q} b_i x^i \in \mathbb{F}_{q^2}[x]$. Moreover, we can assume $a_t = 1$.

Fact 3. 1. $A_0(x) = b_0 + \sum_{i=1}^{t} b_i x^{q/2^i}$.
  2. $b_i = a_i b_t^{q/2^i}$, $i = 1, \dots, t$.

Proof. (*Fact 3*) (1) Via the $\mathbb{F}_{q^2}$-map $x \mapsto x + b_q$ applied to Eq. (9), we can assume $b_q = 0$. Let i be a natural number which is not a power of two and satisfies the condition $3 \le i < q$. Applying D^i to Eq. (9) we have (1) as $D^i y = 0$.

(2) From Item (1) and Eq. (9) we have the following equation:

$$(10) \qquad x^{q+1} + \sum_{i=1}^{t} a_i y^{q/2^i} + \sum_{i=1}^{t} b_i x^{q/2^i} + b_0 = 0 \,,$$

where $a_1 := a \ne 0$. Then, $Dy = x^q + b_t$ and $D^2 y = a_{t-1} x^{2q} + a_{t-1} b_t^2 + b_{t-1}$. Now we want to use Eq. (4); thus we first have to compute $y^{q^2} + y$. Eq. (10) allows us to do the following computations

$$a_1^{2q} y^{q^2} = a_2^{2q} y^{q^2/2} + \sum_{i=2}^{t-1} a_{i+1}^{2q} y^{q^2/2^i} + x^{2q(q+1)} + \sum_{i=0}^{t-1} b_{i+1}^{2q} x^{q^2/2^i} + b_0^{2q} \,,$$

and

$$a_1^q y^{q^2/2} = \sum_{i=2}^{t} a_i^q y^{q^2/2^i} + x^{q(q+1)} + \sum_{i=1}^{t} b_i^q x^{q^2/2^i} + b_0^q \,,$$

so that

$$a_1^{3q} y^{q^2} = \sum_{i=2}^{t-1} (a_2^{2q} a_i^q + a_1^q a_{i+1}^{2q}) y^{q^2/2^i} + a_2^{2q} y^q + a_1^q x^{2q(q+1)} + a_2^{2q} x^{q(q+1)} + a_1^q b_1^{2q} x^{q^2} +$$

$$\sum_{i=1}^{t-1} (a_2^{2q} b_i^q + a_1^q b_{i+1}^{2q}) x^{q^2/2^i} + a_2^{2q} b_t^q x^q + a_2^{2q} b_0^q + a_1^q b_0^{2q} \,.$$

Now, applying $D^{q/2^i}$, $1 \le i < t$, to Eq. (10) and taking into account that $D^\ell = 0$ for $3 \le \ell < q$, we have

$$a_i (Dy)^{q/2^i} + a_{i+1} (D^2 y)^{q/2^{i+1}} = b_i \,,$$

and so, for $1 \le i < t$,

(∗1) $a_i = a_{t-1}^{2^{t-i-1}}$, and
(∗2) $b_i = a_{i+1} b_{t-1}^{q/2^{i+1}}$.

It follows that

$$a_2^{2q} a_i^q + a_1^q a_{i+1}^{2q} = a_2^{2q} b_i^q + a_1^q b_{i+1}^{2q} = 0 \qquad (i = 1, \ldots, t-1) \,,$$

and hence

$$a_1^{3q} y^{q^2} = a_2^{2q} y^q + a_1^q x^{2q(q+1)} + a_2^{2q} x^{q(q+1)} + a_1^q b_1^{2q} x^{q^2} + a_2^{2q} b_t^q x^q + a_2^{2q} b_0^q + a_1^q b_0^{2q} \,.$$

Now, from Eq. (10) together with the following identities coming from (∗1) and (∗2),

- $a_1^{3q+2} = a_2^{2q}$,
- $a_i = a_{i+1}^2 a_{t-1}$, $i = 1, \ldots, t-1$,

- $b_i = b_{i+1}^2 a_{t-1}$, $i = 1, \ldots, t-2$,

we deduce the identity between polynomials in x:

$$a_1^{q+2} a_{t-1} x^{2q(q+1)} + a_1^2 a_2^{2q} a_{t-1} x^{q(q+1)} + a_1^{q+2} a_{t-1} b_1^{2q} x^{q^2} + a_2^{2q} a_{t-1} x^{2q+2} + a_2^{2q} x^{q+1} +$$

$$a_{t-1}(a_2^{2q} b_1^2 + a_1^2 a_2^{2q} b_t^q) x^q + a_2^{2q}(a_{t-1} b_t^2 + b_{t-1}) x^2 + a_2^{2q} b_t x + a_2^{2q}(a_{t-1} b_0^2 + b_0) + a_1^2 a_2^{2q} a_{t-1} b_0^q +$$

$$a_1^{q+2} a_{t-1} b_0^{2q} = a_2^{2q}(x^{q^2} + x)(x^q + b_t) + a_2^{2q}(x^{2q^2} + x^2)(a_{t-1} x^{2q} + a_{t-1} b_t^2 + b_{t-1}).$$

Then, from the coefficients of x^{q^2} we obtain $a_1^{q+2} b_1^{2q} a_{t-1} = a_2^{2q} b_t$. Moreover, since $a_2 \neq 0$ and $a_{t-1} \in \mathbb{F}_{q^2}$, from (∗1) and (∗2) we have that $b_{t-1} = a_{t-1} b_t^2$. In addition, from (∗2) we also have that $b_i = b_{t-1}^{q/2^{i+1}} a_{t-1}^{q/2^{i+1}-1}$, $i = 1, \ldots, t-1$, and Item (2) follows. □

To finish the proof of Claim 1, we apply the $\mathbb{F}_{q^2}$-map $(x, y) \mapsto (x, b_t x + y)$ to Eq. (10). We obtain a relation of type

$$x^{q+1} + \sum_{i=1}^{t} a_i y^{q/2^i} + b_0 + \sum_{i=1}^{t} (a_i b_t^{q/2^i} + b_i) x^{q/2^i} = 0.$$

and Claim 1 follows Fact 3(2).

4. Case $q = 4$. Here, for $q = 4$, we prove the theorem without the hypothesis on Weierstrass non-gaps.

Proposition 2. *An $\mathbb{F}_{16}$-maximal curve $\mathcal{X}$ of genus $g = 2$ is $\mathbb{F}_{16}$-isomorphic to the non-singular model of $y^2 + y = x^5$. In particular, it is $\mathbb{F}_{16}$-covered by the Hermitian curve over $\mathbb{F}_{16}$.*

Proof. We show that $\mathcal{X}$ satisfies the hypothesis in Proposition 1(2). Clearly, $\dim(\mathcal{D}_\mathcal{X}) = 3$ and $m_1(P) \in \{2, 3\}$ for $P \in \mathcal{X}(\mathbb{F}_{16})$. Suppose that $m_1(P) = 3$ for each $P \in \mathcal{X}(\mathbb{F}_{16})$. Then by Lemma 1(2), the $(\mathcal{D}, P)$-orders (resp. $\mathcal{D}$-orders) are 0,1,2 and 5 (resp. 0,1,2 and 4). In addition, for $Q \notin \mathcal{X}(\mathbb{F}_{16})$, the $(\mathcal{D}, Q)$-orders are either 0,1,2 and 4 or 1,2,3 and 4. Then, the following statements hold:

1. the $2\mathcal{D}$-orders are 0,1,2,3,4,5,6,7, and 8;
2. for $P \in \mathcal{X}(\mathbb{F}_{16})$, the $(2\mathcal{D}, P)$-orders are 0,1,2,3,4,5,6,7 and 10;
3. for $P \in \mathcal{X} \setminus \mathcal{X}(\mathbb{F}_{16})$, the $(2\mathcal{D}, P)$-orders are 0,1,2,3,4,5,6,7, and 8.

Thus $\mathrm{Supp}(R) = \mathcal{X}(\mathbb{F}_{q^2})$ and $v_P(R) = 2$ for each $P \in \mathcal{X}(\mathbb{F}_{q^2})$, with R being the ramification divisor associated to $2\mathcal{D}$. Thus

$$36(2g - 2) + 40 = \deg(R) = 2\#\mathcal{X}(\mathbb{F}_{16}) = 2(4(2g - 2) + 25),$$

which implies $28(2g - 2) = 10$, a contradiction. □

5. An $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$, which satisfies the hypothesis of the theorem, is $\mathbb{F}_{q^2}$-isomorphic to $\mathcal{H}/\langle\tau\rangle$, where $\mathcal{H}$ is the Hermitian curve and τ an involution on $\mathcal{H}$. Conversely, let us consider a separable $\mathbb{F}_{q^2}$-covering of curves

$$\pi : \mathcal{H} \to \mathcal{X}\,.$$

Notice that $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal by [La, Prop. 6]. Let g be the genus of $\mathcal{X}$. We have the following

Proposition 3. *In the above situation, suppose that $g > \lfloor\frac{q^2-q+4}{3}\rfloor$. Then $\deg(\pi) = 2$ and $g = \lfloor\frac{(q-1)^2}{4}\rfloor$. In addition,*

1. *$\mathcal{X}$ is the non-singular model of $y^q + y = x^{(q+1)/2}$ provided that q odd*
2. *$\mathcal{X}$ is the non-singular model of $\sum_{i=1}^{t} y^{q/2^i} = x^{q+1}$ provided that $q = 2^t$.*

Proof. Th claim $\deg(\pi) = 2$ follows from the Riemann-Hurwitz formula taking into account the hypothesis on g. Then π has (totally) ramified points: this follows from the Riemann-Hurwitz formula and [FT1]. On the other hand, the hypothesis on g allows us to use [CKT1, Lemma 3.1] and [FGT, Prop. 1.5] to conclude that

$$m_1(P) < m_2(P) \le q < m_3(P) \qquad \text{for each } P \in \mathcal{X}\,.$$

Let $Q_0 \in \mathcal{H}$ be totally ramified for π and set $P_0 := \pi(Q_0)$. Then the Weierstrass non-gaps at Q_0 less than or equal to $2q$ are

$$\text{either} \qquad q, 2q-1, 2q \qquad \text{or} \qquad q, q+1, 2q\,.$$

It follows that $m_2(P_0) = q$ and that $2m_1(P_0) \in \{q, q+1\}$ (see e.g. [T, proof of Lemma 3.4]). Now if q is odd, $m_1(P_0) = (q + 1)/2$ so that $m_3(P_0) = q + 1$; hence $P_0 \in \mathcal{X}(\mathbb{F}_{q^2})$ and (1) follows from [FGT, Thm. 3.1].

If q is even, we claim that P_0 can be chosen in $\mathcal{X}(\mathbb{F}_{q^2})$. To see this, as $\deg(\pi) = 2$, for each $Q \in \mathcal{X}(\mathbb{F}_{q^2})$ the product formula gives the following possibilities:

1. $\#\pi^{-1}(Q) = 2$ and $\pi^{-1}(Q) \subseteq \mathcal{H}(\mathbb{F}_{q^2})$;
2. $\#\pi^{-1}(Q) = 1$ and $\pi^{-1}(Q) \in \mathcal{H}(\mathbb{F}_{q^2})$;
3. $\#\pi^{-1}(Q) = 1$ and $\pi^{-1}(Q) \in \mathcal{H}(\mathbb{F}_{q^4})$.

Since $\mathcal{H}(\mathbb{F}_{q^4}) = \mathcal{H}(\mathbb{F}_{q^2})$ we have that (3) is empty if $Q \in \mathcal{H}(\mathbb{F}_{q^4}) \setminus \mathcal{H}(\mathbb{F}_{q^2})$. Since $2\#\mathcal{X}(\mathbb{F}_{q^2}) > \#\mathcal{H}(\mathbb{F}_{q^2})$, the claim follows.

Finally we get $2m_1(P) = q$ and the result follows from Proposition 1. $\square$

References

[ACGH]   E. Arbarello, M. Cornalba, P.A. Griffiths, and J. Harris, Geometry of Algebraic Curves, Vol. I, Springer-Verlag, New-York, 1985.

[Cas]   G. Castelnuovo, Ricerche di geometria sulle curve algebriche, *Atti. R. Acad. Sci. Torino* **24**, 196–223 (1889).

[CHKT]   A. Cossidente, J.W.P. Hirschfeld, G. Korchmáros and F. Torres, On plane maximal curves, Compositio Math., to appear.

[CKT1]   A. Cossidente, G. Korchmáros and F. Torres, On curves covered by the Hermitian curve, J. Algebra, to appear.

[CKT2]   A. Cossidente, G. Korchmáros and F. Torres, On curves covered by the Hermitian curve, II, (math.AG/9807166), preprint.

[FGT]   R. Fuhrmann, A. Garcia and F. Torres, On maximal curves, *J. Number Theory* **67**(1), 29–51 (1997).

[FT1]   R. Fuhrmann and F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math.* **89**, 103–106 (1996).

[FT2]   R. Fuhrmann and F. Torres, On Weierstrass points and optimal curves, *Rend. Circ. Mat. Palermo Suppl.* **51**, 25–46 (1998).

[GT]   A. Garcia and F. Torres, On maximal curves having classical Weierstrass gaps, (math.AG/9801106), submitted.

[G-Sti-X]   A. Garcia, H. Stichtenoth and C.P. Xing, *On subfields of the Hermitian function field*, preprint (1998).

[G-Vi]   A. Garcia and P. Viana, Weierstrass points on certain non-classical curves, *Arch. Math.* **46**, 315–322 (1986).

[Geer-Vl1]   G. van der Geer and M. van der Vlugt, How to construct curves over finite fields with many points, *Arithmetic Geometry* (Cortona 1994), F. Catanese Ed., Cambridge Univ. Press, Cambridge, 169–189, 1997.

[Geer-Vl2]   G. van der Geer and M. van der Vlugt, Generalized Reed-Muller codes and curves with many points, Report W97-22, Mathematical Institute, University of Leiden, The Netherlands, alg-geom/9710016.

[Go]   V.D. Goppa, Algebraic-geometric codes, *Math. USRR-Izv.* **21**(1), 75–91 (1983).

[He]   A. Hefez, Non-reflexive curves, *Comp. Math.* **69**, 3–35 (1989).

[Ih]   Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokio* **28**, 721–724 (1981).

[K]   T. Kato, On Weierstrass points whose first non-gaps are three, *J. Reine Angew. Math.* **316**, 99–109 (1979).

[La]   G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, *C.R. Acad. Sci. Paris* **305**, Série I, 729–732 (1987).

[Ra]   J. Rathmann, The uniform position principle for curves in characteristic p, *Math. Ann.* **276**, 565–579 (1987).

[R-Sti]   H.G. Rück and H. Stichtenoth, A characterization of Hermitian function fields over finite fields, *J. Reine Angew. Math.* **457**, 185–188 (1994).

[Sti-X]   H. Stichtenoth and C.P. Xing, The genus of maximal function fields, *Manuscripta Math.* **86**, 217–224 (1995).

[SV]   K.O. Stöhr and J.F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.* **52**, 1–19 (1986).

[T]   F. Torres, On certain N-sheeted coverings of curves and numerical semigroups which cannot be realized as Weierstrass semigroups, *Comm. Algebra* **23**(1), 4211–4228 (1995).

IMPA, Est. Dna. Castorina 110, Rio de Janeiro, 22.460-320-RJ, Brazil

E-mail address: `miriam@impa.br`

IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP, Brazil

E-mail address: `ftorres@ime.unicamp.br`